Activity 3: Management report justifying the solution

Security requirement:

The network will only allow secure connections.

Protection measure 1:

Attack through remote access, attack on network through Wi-Fi access and misconfigured firewall.

Using a port scanner software will find open ports on the network, any ports that are open and not being used are vulnerable as a cybercriminal could also find these ports by using a port scanner, attackers can connect to these unused ports allowing them to send packages that can be harmful into the network.

Closing these ports will prevent attackers from connecting and gaining unauthorised access so this protection measure is effective in only allowing secure connections.

An alternative measure would be to only use wired connections on the network as it would prevent attackers from connecting to the ports wirelessly, this would be ineffective as the development plan states that both staff and visitors must be able to connect using mobile devices.

Security requirement:

Preventing malware from infecting the system and causing damage to the network.

Protection measure 1:

Attack through remote access, attack on network through Wi-Fi access and misconfigured firewall.

The firewall needs to be correctly configured to prevent suspicious files from entering the network, this will prevent the risk of a virus making its way onto the network. The firewall will also be configured to block suspicious files from being opened/ executed on devices connected to the network, this again prevents the risk of a harmful file causing damage to the network.

The router and firewall must be kept up to date to allow the firewall to recognise new malware that has been identified, if the firewall is not kept updated an attacker could plant a new virus onto the network that won't be recognised as a threat by the firewall.

Protection measure 7:

Phishing and Malicious software.

Having staff effectively trained means that they will not accidently allow malware into the network and that they are more aware on how to prevent a virus from getting onto the network and causing damage.

An alternative measure would be to disable all files that are not preinstalled onto devices, this would prevent any malware from being opened on a device on the network but will prevent staff from using software they may need access to.

Security requirement:

To keep confidential information safe and secure.

Protection measure 2:

Attack on or theft of confidential information and Misconfigured access levels.

Having different logins for members of staff means only the correct users are granted access to the files they need. This ensures that a visitor cannot log into the network and access all the files on the network. Access levels also enforces this as it prevents guest accounts from accessing staff files. If everybody on the network was granted access to all files, then confidential information won't be protected against a cyber-criminal leaking the information.

Making sure that staff use a VPN when accessing the network from home protects the information being sent and received over the network as all the info will be encrypted meaning if an attacker intercepts the data being sent, they won't be able to read or understand any of the data.

Protection measure 4:

Attack on unprotected/ misconfigured access points and Unprotected RJ45 ports in server room.

Installing port blockers or port guards onto unused ports on a network prevents an attacker from connecting their device to the port to gain access to the files on the network.

Alternative measures would be to have all confidential information store on one device on the network which can be protected and secured or having only hard physical copies of the information.

The measures I have used are more appropriate as the development plan states that freelance trainers and assessors will need access to appropriate secure areas of the network from home or work locations.

Security requirement:

Preventing unauthorised access and damage to hardware on the system.

Protection measure 3:

Having card scanners on each side of the doors means that BCTAA can ensure that only authorised users have access to the building and they will know who is within the building if a data breach does occur. The doors will also be locked protected hardware on the inside from being tampered with.

Protection measure 5:

Locating the server and hardware of the system in a separate secure room helps BCTAA in protecting the equipment physically. Having the Cat6 cables protected through each room it passes through protects it from public access as an attacker cannot then destroy the cables, taking down the network.

An alternative measure would be to have staff members located outside every room to grant access to other staff with ID, this may be ineffective as it would be costly to pay staff to guard each room every day.

Security requirement:

Ensuring that the security of the network is of a high standard.

Protection measure 6:

To ensure that all passwords used on the network are strong and secure, a password policy will be put in place that requires each password to be:

- Over 8 characters long.
- Include numerical characters.
- Include at least one upper case character.
- Updated every 5 months.
- Not be a password used before.

This ensures that all passwords are strong and not easily guessed by brute force software used by hackers to try gain unauthorised access into a system.

An alternative measure would be to have one master secure password for all devices on the network, this could prove inappropriate as if this one password is breached by an attacker they would have access to all devices on the network.